TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2€
n.170
HACKER JOURNAL
www.hackerjournal.it
ARP SPOOFING
COME SPIARE UNA LAN
MOBILE
iPHONE DOPATO
PRIVACY
LA LEGGE CHE NON DEVE PASSARE
INTERVISTA A MATT KNOX
STORIA DI UN ADWARE PROGRAMMER
SPY WORLD
VIAGGIO NEI CIFRARI DELL'FBI
METTITI ALLA PROVA
CRACKING
AGGIRATI I CAPTCHA DI MEGAUPLOAD
QUATTORD. ANNO 9 - N° 170 - 19/25 FEBBRAIO 2009 - € 2,00
WLF PUBLISHING

Anno 9 – N.170
19/25 febbraio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata
al Tribunale di Milano
il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

La saggezza della Rete

"Non vale la pena avere la libertà se questo non implica avere la libertà di sbagliare".
Gandhi

Navigando nella Rete mi sono imbattuto in un blog appena nato (http://attaccabrighedigitale.wordpress.com) che mi ha molto colpito. Credo abbia ben capito lo spirito hacker, anche se non è gestito da un hacker e non parla di hacking. Ecco alcuni estratti che più mi hanno fatto riflettere e che spero sortiscano lo stesso effetto in te che leggi:

…Questo Blog è un semplice deposito di quello che ho raccolto e raccoglierò sul tema del mercato digitale, della cultura digitale e del diritto d'autore. Cioè della nostra Libertà di espressione e informazione e di come essa possa essere garantita o limitata dalle leggi sulle merci digitali. Io non sono un esperto del tema. Sono la collaboratrice domestica della Rete che cerca di tenere in ordine quello che persone più colte e intelligenti di me pensano, scrivono e dicono. Perché mi darebbe molto fastidio che la mia Libertà venisse limitata per ignoranza, stupidità o cupidigia.

A proposito di pirati

Quando si parla di Pirateria bisognerebbe parlare dei Pirati. Essere un Pirata non vuol dire semplicemente essere un ladro. Anzi, un Pirata, per definizione, non è un ladro. È un ribelle, un rivoluzionario, il motore del cambiamento della società. Infatti sarebbe più corretto parlare di Furto Digitale e non di Pirateria Digitale: è un distinguo culturalmente molto importante. Le parole hanno un significato preciso, fare confusione con le parole vuol dire fare confusione con le idee. Di Pirati hanno scritto autori curiosi e informati. Li segnalo a voi nei Documenti e nei Link di questo Blog perché possiate leggerli e criticare le loro idee, sottoscriverle, o farvene di vostre. Questo Blog è stato compilato per dare un contributo culturale ampio alla discussione e consentire a tutti di accedere facilmente alle informazioni.

Compito per questo mese:
se non lo hai già apri un blog. Altrimenti manda un post a un blog che ti piace o che ti ha colpito. La discussione e il confronto di idee sono alla base della cultura hacker.

Il Coccia

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE
Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Un nuovo organizzatore per Capture The Flag

Dopo quattro anni di ottimo lavoro, Kenshoto ha preferito lasciare il testimone a qualcun altro. Da questo momento, quindi, l'organizzazione di DefCon sta cercando un nuovo partner in grado di organizzare, ospitare e gestire la competizione che più di tutto ha contribuito alla diffusione del nome della manifestazione. Nelle quattro passate edizioni, gli organizzatori di Kenshoto sono riusciti a elevare notevolmente il livello del contest, con nulla di scontato e molto divertimento per tutti. Le proposte sono aperte, ma niente è dato per assunto. L'organizzazione di DefCon si assumerà il compito di vagliare con attenzione tutte le applicazioni: inutile dire che i requisiti sono necessariamente di alto livello, non è una posizione che tutti possono occupare.

Occorre una buona struttura di base: scherzosamente DefCon ricerca "una grande multinazionale cattiva, un gruppo autonomo e nefasto di geni hacker o un'organizzazione governativa fantasma da qualunque parte del mondo", ma ciò non è molto distante dalla realtà. Per Capture the Flag infatti occorre più che genialità, occorre avere le cosiddette... La struttura del contest è completamente aperta a tutte le soluzioni, l'importante è che sia tosta. Si possono creare quest singoli o collaborativi, prevedere delle eliminatorie per selezionare i gruppi che potranno partecipare, usare qualsivoglia strumento tecnologico (anzi, più ce n'è e meglio è) tra cui computer, saldatori, tecnologie varie, qualunque cosa. Si può prevedere anche una struttura distribuita dei partecipanti (non solo presenti fisicamente alla manifestazione, ma anche esterni via VPN), l'importante è che la rete su cui si svolge il contest sia autonoma e completamente slegata dalla rete della manifestazione e che la stessa non vada a interferire con la rete pubblica (Internet). Sono richieste anche assoluta imparzialità ed estrema chiarezza sia nell'esporre il progetto allo staff di DefCon, sia nel trasmettere il regolamento ai partecipanti. Tutto deve essere attentamente pianificato e documentato, nulla può essere lasciato all'improvvisazione o al caso.

Se siete consci di quanto impegno questa organizzazione richieda, avete alle spalle un buon gruppo di lavoro che possa supportare le vostre idee, accettate tutte le regole imposte dallo staff e (soprattutto) avete fantasia e l'adeguata conoscenza, trovate informazioni e le modalità di adesione sul forum di DefCon, all'indirizzo https://forum.defcon.org/showthread.php?t=10130.

▲ *Alcuni elaborati in concorso per il manifesto pubblicitario di DefCon del 2008.*

BLUETOOTH PER IPHONE

Scambiarsi dati, foto, video e altri documenti con il proprio iPhone via Bluetooth presto non sarà più un problema. Non è certo merito di Apple, che per motivi ancora misteriosi ha limitato l'uso del bluetooth su iPhone alla sola trasmissione audio (impedendogli di comunicare con altri dispositivi bluetooth), ma della bravura di MeDevil, un programmatore italiano che ha "aggirato" il blocco imposto dal produttore, realizzando un software in grado scambiare liberamente ogni tipo di dati con altri device dotati di Bluetooth. Il rilascio dell'applicazione per gli iPhone sbloccati, che dovrebbe vedere la luce in questi giorni, rappresenta un altro passo importante nella "liberalizzazione" di un telefono nato con troppi vincoli e restrizioni: del resto chi può impedire al legittimo proprietario di un prodotto di farci quello che desidera?

PROVA DI MATURITÀ ...DI YOU TUBE

Il Ministro della Pubblica Istruzione, Maria Stella Gelmini, ha comunicato, come solitamente avviene in questo periodo, le materie per la seconda prova dell'esame di maturità 2009. La cosa particolare è che l'ha fatto con un video su Youtube, cogliendo alla sprovvista professori e studenti. Youtube non è nuovo ad essere utilizzato come strumento "istituzionale", tanto è vero che anche il Presidente degli Stati Uniti, Barack Obama, sfrutta ormai da tempo il suo canale video per comunicare velocemente con i suoi elettori. È bello quindi che, seppure con sensibile ritardo, anche l'Italia abbia capito l'importanza di queste nuove tecnologie. Grazie quindi al Ministro Gelmini per aver usato la Rete per comunicare le materie per la maturità: finalmente lo stesso mezzo che da anni gli studenti utilizzano per sapere in anticipo le tracce degli esami!

VISTA HOME BASIC... NON È VISTA

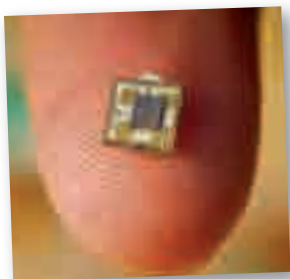
Gioiscano gli utenti di Windows Vista Home Basic: la loro versione di Vista, non è Windows Vista. Sembra una notizia paradossale ma è quanto è emerso dagli sviluppi di una class action americana (ovvero una causa intentata da più utenti) contro Microsoft per il famigerato bollino "Vista Capable" applicato a moltissimi computer in vendita nel 2006 alla vigilia dell'uscita di Windows Vista nei negozi. In pratica gli utenti contestano la correttezza del bollino, dal momento che in molti computer Vista Capable in realtà è stato possibile installare solo la versione Home Basic priva dell'interfaccia Aero e di altre funzioni avanzate proprie di Windows Vista. Addirittura, secondo alcuni documenti portati al processo, Microsoft stessa non considerava Home Basic come una versione di Vista a tutti gli effetti, tanto è vero che il nome di questo sistema operativo doveva essere originariamente Windows Home Basic (senza Vista). Ora starà ai giudici stabilire se ci sono gli estremi per un risarcimento, mentre a noi resta solo una considerazione: visti i problemi e lo scarso successo di Vista, probabilmente chi ha potuto installare sul suo PC solo Home Basic, può ritenersi davvero fortunato!

HOT NEWS

MICROSOFT PROLUNGA LA DISTRIBUZIONE DI WINDOWS 7

Avete tempo fino al 12 febbraio per scaricare la prima Beta pubblica di Windows 7, il nuovo sistema operativo di Microsoft previsto per la fine dell'anno. Windows 7 è, a detta di molti, decisamente più affidabile, leggero e performante rispetto a Vista, per cui vale la pena provarlo. Se non doveste riuscire a scaricarlo per tempo, non preoccupatevi: oltre ai canali "paralleli" (Bittorrent, Emule e altri), Microsoft ha promesso che presto rilascerà una seconda versione per tutti coloro che si sono persi la prima. Insomma, tutti potranno provare in anteprima Windows 7 prima del suo rilascio definitivo: vista la proverbiale riservatezza di Microsoft sui sistemi operativi in versione beta, c'è da chiedersi se questo non sia un atto di scuse per averci costretto a utilizzare Windows Vista da 2 anni a questa parte.

UN CHIP A 60 GHZ PER LA COMUNICAZIONE WIRELESS

La tecnologia fa progressi sempre più rapidi soprattutto per quanto riguarda i dispositivi per la comunicazione Wireless. Questa vota a fare notizia è la realizzazione da parte dei tecnici dell'istituto di tecnologia della Georgia di un chip in grado di inviare e ricevere dati alla velocità di ben 60 Ghz. Il piccolo processore, delle dimensioni di un coriandolo, può scambiare dati con altri dispositivi nel raggio di 10 metri alla velocità di oltre 5 Gbps e, viste le dimensioni contenute, potrà essere inserito facilmente nei telefoni di nuova generazione… se tutto va bene tra più di un anno! Non ve l'abbiamo detto? L'ente internazionale che regola la concessione delle frequenze ancora non ha approvato le trasmissioni sui 60GHz e servirà prima una tavola rotonda con governi, produttori e esperti per preparare un piano di utilizzo di questi nuovi dispositivi. Farà la fine del Wi-Max?

KIT R4 FUORILEGGE

Buone notizie per Nintendo (e meno buone per tutti coloro che non hanno ancora modificato il loro DS): il tribunale di Milano ha condannato l'azienda di Firenze PCBox per aver realizzato e venduto il suo kit di modifica per Nintendo DS chiamato R4 Revolution: questo dispositivo (in pratica una cartuccia per la console opportunamente modificata) permetteva ai possessori di Nintendo DS di avviare giochi non originali semplicemente salvandoli nella sua memoria interna. Lo scopo dell'R4, hanno spiegato i produttori, era solo quello di creare legittime copie di backup dei giochi per poterli avere tutti disposizione in un'unico supporto. Inoltre, secondo la difesa, ognuno è libero di fare quello che vuole della propria console. Peccato che il giudice non sia stato dello stesso parere, e abbia deliberato in favore di Nintendo. Evidentemente il magistrato non fa parte della categoria di persone che in casa hanno almeno un programma, un film o un gioco copiato! Chi è senza peccato…

iWork sui torrent, ma con il virus!

Il 5 gennaio scorso, Apple ha presentato la sua nuova suite di programmi per ufficio iWork 2009, e già pochi giorni dopo circolavano le prime copie del programma sui canali P2P: una manna dal cielo per molti "scaricatori" che però non si sono accorti che all'interno del programma alcuni ingegnosi criminali informatici avevano inserito un pericolosissimo trojan. OSX.Trojan.iServices.A, questo il nome della minaccia, utilizza l'installer del programma per contagiare il sistema: una volta in memoria, questo virus apre le porte a un server remoto che può avere libero accesso al vostro Mac per rubare dati e informazioni sensibili. Ancora non sono chiari gli obiettivi degli autori del virus ma la sua diffusione è stata agevolata dal fatto che molti utenti Mac non ritengono necessaria l'installazione di un antivirus per OSX visto lo scarso numero di minacce per questo sistema operativo. Illusi!

ALLARME CLICKJACKING

La lotta per la sicurezza della navigazione che coinvolge praticamente tutti i browser esistenti, ha un nuovo nemico: si chiama clickjacking e non è altro che l'ennesimo stratagemma per spingere gli utenti su siti che non vorrebbero mai visitare. In pratica, grazie ad un bug nella gestione dei javascript, i pirati possono collegare il clic su un qualsiasi elemento html ad un collegamento verso una pagina web, un banner o il download di un programma, senza che gli utenti possano accorgersene per tempo. Il fenomeno si sta diffondendo a macchia d'olio e sempre più siti al limite della legge, utilizzano tecniche di clickjacking per inviare i visitatori su portali di sponsor, iscriverli a newsletter (per inviare spam) e altro ancora. Per il momento si tratta di minacce innocue e preso i principali browser dovrebbero rilasciare una patch per "tappare" il buco nello script. Tuttavia non possiamo prevedere se la protezione durerà oppure i pirati saranno capaci di modificare i loro software di clickjacking per puntare ai nostri dati sensibili!

NOKIA MINACCIA LA FINLANDIA E I SUOI DIPENDENTI

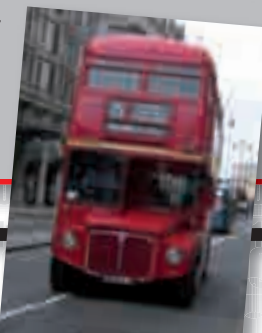
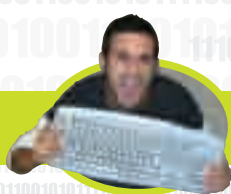
Da anni Nokia è sinonimo di efficienza e tecnologia finlandese, tuttavia presto il popolare produttore di telefonini potrebbe abbandonare la sua patria e trasferirsi altrove. Il motivo? Le leggi finlandesi non consentono di spiare le e-mail dei dipendenti! Tutto inizia da una classica storia di spionaggio industriale: Nokia sospetta che un suo dipendente passi informazioni riservate alla concorrenza, per cui inizia a spiare la sua casella di posta per provare il "tradimento". Per tutta risposta, il dipendente, una volta accortosi della cosa, denuncia l'azienda per violazione della privacy. Insomma, tutto nella norma, se non fosse che, per la legge finlandese è il dipendente ad avere ragione.

Per questo motivo Nokia inizia a fare pressioni sul governo per cambiare la legge vigente, minacciando di levare le tende nel caso in cui la nuova legge (che è già stata ribattezzata dalla stampa Nokia Lex) non venisse approvata. Ancora non sappiamo come si risolverà la bagarre, ma ancora una volta gli interessi economici rischiano di prevalere sui diritti dei cittadini.

L'INGHILTERRA TASSA IL P2P

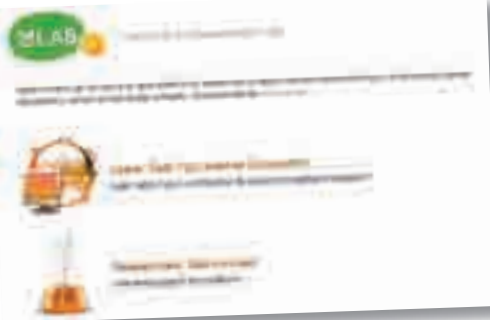
Pagare tutti, pagare... di più. Per fronteggiare la crisi delle etichette discografiche e delle major che vedono nella pirateria la sola causa delle loro magre entrate (non i costi alti a cui vendono film e musica, non la distribuzione insensata, non le politiche di mercato... solo la pirateria), il Ministro della Cultura britannico, Andy Burnham, ha presentato al parlamento una proposta di legge che prevede un aumento annuo di 20 sterline sugli abbonamenti a internet come "risarcimento" alle major per chi scarica attraverso canali P2P. Insomma, che scarichino o no, gli utenti Inglesi dovranno pagare un risarcimento alle aziende di intrattenimento. La proposta di Burnham, tuttavia, fa parte di un progetto di legge ancora più articolato che, si dice, potrebbe obbligare i provider ad applicare tariffe di abbonamento diverse a seconda dei contenuti scaricati dai loro abbonati: in barba alla britannica privacy.

FIREFOX CI SPIA... MA PER AIUTARCI!

Spiare le nostre attività su internet è sempre stata una passione non solo di pirati e malintenzionati, ma anche di società di tutto rispetto come Microsoft, Apple e altri. Tuttavia per una volta potrebbe farci comodo venire spiati da Firefox. I programmatori del popolare browser infatti hanno rilasciato un plugin aggiuntivo chiamato Web pilot il cui compito è quello di raccogliere (in modo

IL DIGITALE TERRESTE È NATO GIÀ MORTO!

Per le tecnologie legate alle trasmissioni televisive il 2009 doveva essere un anno fondamentale: a partire dal 1 gennaio infatti la Sardegna è diventata la prima regione ad abbandonare il segnale analogico per il "più moderno" digitale terrestre. Una bella notizie se non fosse che questa tecnologia presenta dei limiti che probabilmente ne condanneranno il futuro in pochi anni. Per prima cosa, il sistema di trasmissione si affida comunque ai vecchi ripetitori analogici che quindi conservano i problemi di ricezione del segnale legati alla morfologia del nostro Paese. Il secondo, se vogliamo, è ancora più preoccupante: la portata del segnale digitale infatti è molto più bassa rispetto a quella del satellitare. Di conseguenza, se oggi con poche emittenti che trasmettono in digitale tutto fila liscio, cosa succederà quando altri operatori accederanno alle frequenze del digitale terrestre ingolfando tutta la banda disponibile? Non è un caso che negli ultimi tempi sono apparsi sul satellite nuovi canali Mediaset, vera pioniera del digitale

P2P LIMITATO? GOOGLE LO SCOPRE

Avete un'ADSL da 7 mega ma scaricate a 30k al secondo? Probabilmente la colpa è del vostro provider. Circa un anno fa fece scalpore la notizia che alcuni provider riducevano la banda del traffico effettuato tramite canali di P2P, senza avvertire i propri utenti.

Questo sistema non è consentito dalle leggi sulla trasparenza delle offerte Internet e se finora non era possibile scoprire la subdola mossa del provider, oggi grazie a Google potete farlo. M-lab (www.measurementlab.net), nato dalla collaborazione di Google con l'Open Technology e il PlanetLab Consortium, presenta Glasnost, lo strumento capace di scoprire se ci sono dei sistemi che ci impediscono di scaricare ciò che vogliamo in santa pace.

UN LINUX TARGATO INTEL

Forte della produzione del fortunato processore Atom per i nuovi netbook, Intel ha deciso di sviluppare autonomamente un nuovo sistema operativo open source per sfruttare al massimo le potenzialità di queste nuove CPU. Moblin è un sistema operativo molto compatto (occupa poco meno di 300 Mb) appositamente pensato per stare comodamente sui veloci, ma non capientissimi, dischi a stato solido SSD. Inoltre, secondo gli sviluppatori, consentirà agli utenti di essere operativi in una manciata di secondi dall'accensione. Chi vuole provare la versione Alpha può collegarsi al sito moblin.org per scaricarla.

anonimo) le abitudini dei navigatori per migliorare i servizi e l'interfaccia del browser nelle prossime release. Si tratta comunque di un'invasione della privacy, ma almeno i programmatori di Mozilla lo rivelano pubblicamente e ci mettono a disposizione anche i risultati delle varie ricerche da consultare gratis.

TUTTI D'ACCORDO SUGLI HARD DISK CRIPTATI

Il Trusted Computing Group (CTG) un'organizzazione che riunisce i maggiori produttori di hard disk del mondo, ha finalmente ufficializzato il primo standard di criptazione per i dischi fissi.

Aziende del calibro di Fujitsu, Western Digital, Hitachi, Seagate e altri ancora sono riusciti a raggiungere un accordo per la futura realizzazione di hard drive che integrano nativamente il protocollo di codifica AES 128 o 256 bit (a seconda del grado di sicurezza richiesta). Entro pochi anni, nessuno potrà rimuovere e ricollegare un hard disk o una chiavetta USB, senza dover poi digitare la password per poter accedere ai propri documenti... almeno finché gli hacker non troveranno il modo di forzare la protezione!

COME LO FECI

L'esperienza di Matt Knox, programmatore di adware per Direct Revenue

L'adware è uno dei tormenti più fastidiosi per chi lavora con il computer: per poter usare gratuitamente un programma, spesso siamo costretti a installare il software di un "partner commerciale" del produttore. Questo si incarica di esaminare il nostro comportamento sul Web per fare in modo che i banner pubblicitari mostrati rispecchino i nostri interessi. Per alcuni sta bene così, per altri avere una spia che non si sa che tipo di informazioni trasmetta e a chi non sta bene per niente.
Matt Knox è uno dei programmatori più conosciuti di software di questo tipo e, recentemente, ha rilasciato un'intervista molto interessante al blog sulla sicurezza Philosecurity.org.

:: Perché programmare adware?

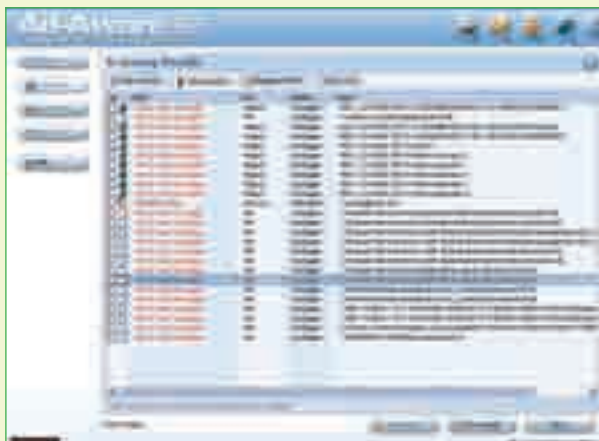
Ciò che traspare dalle parole di Matt è che non si tratta di una scelta personale: uno fa il programmatore, viene assunto da una compagnia e si prende carico dei compiti che gli vengono assegnati, che possono comprendere anche la creazione di adware. Nel suo caso non si è trattato di una richiesta chiara e immediata: il lavoro di Matt è stato indirizzato verso adware piuttosto intrusivo semplicemente partendo da piccole richieste e aggiungendo a poco a poco richieste sempre più specifiche. Il risultato è un software che non solo si comporta come un normalissimo adware, ma è in grado anche di verificare la presenza sul PC di virus che ostacolano il funzionamento del programma e di software di altre compagnie concorrenti per eliminare entrambi dal computer dell'ignaro utente. Una guerra, insomma, combattuta in sordina a nostre spese.

Matt Knox, programmatore adware. Reo confesso ma non pentito?

E Matt afferma che è estremamente facile indurre qualcuno a fare qualcosa di veramente cattivo non presentandola nella sua interezza, ma spezzettandola e chiedendola un frammento alla volta.

:: Come arriva sui nostri PC

Direct Revenue intanto non lo chiama "adware": la compagnia buona che fa soldi sulla pubblicità mirata lo chiama "software supportato da pubblicità". Significa che produce un software, per esempio un salvaschermo o un programmino di utilità, e poi lo collega con le proprie funzioni specifiche. Quindi lo offre gratuitamente al pubblico, in cambio di informazioni sulle loro preferenze, per bombardarli poi di pubblicità mirata.

Ma ci sono anche aziende "cattive": queste non dichiarano apertamente che il proprio programma contiene un adware, ma sfruttano falle della sicurezza di Windows per installarlo all'insaputa dell'utente. A difesa di Direct Revenue, Matt spiega che non è stata mai adottata una linea di condotta simile: anzi, nel momento in cui analizzando software di propri partner trovavano exploit simili, rescindevano il contratto seduta stante. Una nota dolente però rimane: questi software tendono a rimanere installati anche rimuovendo l'applicazione principale, secondo un principio che i loro sviluppatori chiamano "persistence of installation". L'adware continua a compiere il proprio mestiere anche disinstallando il programma con cui è stato distribuito e fa in modo di reinstallarsi ogni volta che un antivirus rimuove i suoi componenti.

Il popolare programma anti-adware AdAware di Llavasoft. Non sempre rimuovere tutto è salutare...

Impossibile quindi, per un utente normale, liberarsi del software indesiderato, a meno che non si segua una procedura macchinosa che comporta visitare un particolare sito Web, rispondere a un modulo che chiede i motivi per cui si vuole rimuovere l'adware e scaricare infine un programma apposito che effettivamente lo rimuove. Il guaio è, spiega Matt, che per evitare di installarsi di nuovo su una macchina da cui è stato rimosso l'adware inserisce un'apposita chiave del registro, che però spesso viene rimossa dagli antivirus. Il risultato è che nel giro di breve tempo si rischia di nuovo "l'infezione".

Spesso l'adware sfrutta falle del browser per mostrare annunci pubblicitari anche quando stiamo facendo altro.

:: Come si nasconde

Innanzitutto bisogna dire che la maggior parte dell'adware colpisce Internet Explorer, per due sostanziali motivi. Primo, gli utenti di IE costituiscono da soli la maggior parte del mercato; secondo, di solito sono gli utenti meno accorti o che non conoscono il PC, e non sanno (o non se ne interessano) che IE stesso è afflitto da mille problemi e falle di sicurezza. Matt ha usato proprio una di queste debolezze: sfruttando il Browser Helper Object di IE il suo adware controllava che tutto fosse a posto interrogando la macchina ogni 10 secondi circa. Se qualcosa mancava, lo installava di nuovo e il gioco era fatto. Con l'aiuto di un programmino di installazione poi le cose si fanno più semplici: si possono scrivere chiavi di registro per controllare la presenza dei processi desiderati e in caso reinstallarli, e si può deporre un piccolo eseguibile. È ingegnoso come questo eseguibile venga nascosto: si prende l'indirizzo MAC della scheda di rete, si codifica con DEC, si prendono i primi sei od otto caratteri e si usano per il nome del file. Così esiste un eseguibile per ogni computer, difficile da individuare anche salvato sempre nella stessa posizione. Anche la firma MD5 del file è sempre la stessa. Per ovviare a questo problema, il programma viene "mischiato" un po': si prendono le funzioni incluse e le si salva in altre posizioni del file, mantenendolo eseguibile, ed ecco che anche le firme proprie del software vengono modificate. Impossibile quindi individuarlo con un antivirus o un programma simile.

:: Pentito e redento?

In realtà, non è colpa di Matt né degli altri programmatori se oggi l'adware per veicolare pubblicità mirata è una prassi così diffusa, ma piuttosto delle aziende che li pagano. In più, Matt afferma che il suo software ha rimosso più virus e altri adware di quante volte sia stato installato, finendo così a fare del "bene". Quello che è certo è che Matt è comunque un programmatore onesto e trasparente, oltre che brillante, e ci ha dato modo di conoscere meglio il funzionamento intimo di un adware.

Ecco come le nostre vite sono controllate dal demone commerciale dei nostri tempi

PECORE COMMERCIALI

Più ci addentriamo nella crisi di cui tutti i telegiornali parlano, più ci invitano a consumare per far riprendere l'economia. Più consumiamo, ovviamente, più spendiamo, e spesso siamo anche invogliati a farlo da un miraggio che ormai qualunque esercizio commerciale crea per attirare nuovi clienti e ottenere la loro fedeltà: le tessere a punti che offrono sconti o premi. Da consumatori anonimi diventiamo consumatori schedati, studiati e, come tante belle pecore nell'ovile, ci adattiamo adeguando i nostri consumi a quello che "loro", demoni commerciali il cui unico scopo è fare soldi e non offrire servizi, pensano che sia meglio per noi. Ça va sans dir, non è mai veramente meglio per noi quanto lo è per loro...

:: Tecniche di allevamento

Ormai tutti sappiamo bene che nulla, nell'ambito di un esercizio commerciale, è lasciato al caso: non ci riferiamo tanto al piccolo negozietto di quartiere (che comunque è destinato a scomparire e a rimanere solo un ricordo) quanto al grande supermercato e al centro commerciale. Non serve quindi perderci troppo tempo, basta rimarcare il fatto che la disposizione dei prodotti è studiata per mettere in risalto quelli più costosi (e con più margine di guadagno per chi li vende) e nei punti più difficili da vedere e/o raggiungere quelli più a buon mercato (e anche qui bisogna valutare bene quanto questi ultimi valgano meno dei primi) e che il percorso stesso, completamente guidato, tra le corsie del supermercato è frutto di studi sociologici e non un semplice fatto pratico/estetico: entriamo e troviamo musica diffusa a livello quasi subliminale, studiata per il target più presente in un determinato orario, siamo investiti dall'esplosione di colori di frutta e verdura fresche che spezzano dal grigiore dell'esterno e invogliano a comprarle; il percorso va da destra a sinistra per seguire la naturale inclinazione di una popolazione in maggior parte destrorsa e la disposizione dei diversi tipi di prodotti è tale che per evitare di fare macelli nel carrello percorriamo l'intero percorso almeno tre volte). Ciò che ci

interessa ora è notare che girando tra le corsie troveremo certamente particolari offerte e sconti di cui possiamo beneficiare solamente se siamo titolari della famigerata tessera. E alla fine ci caschiamo: se siamo economicamente indipendenti (e con questo intendo che lavoriamo e ci occupiamo da soli delle nostre spese) abbiamo nel portafoglio almeno qualcuna di queste tessere, che siano del benzinaio piuttosto che del supermercato.

:: Lo specchietto per le allodole

Recuperiamo dal portafoglio una di queste tessere e studiamola un attimo, e vediamo come molti aspetti del loro utilizzo ci sfuggano e possono essere usati non proprio a nostro vantaggio.
Prendo in esame una tessera a caso, di colore verde e con una bella fragola disegnata su una sua faccia, ma potrebbe essere una qualsiasi altra tessera. In apparenza è piuttosto anonima: da un lato solo il simbolo del frutto e il nome della catena di supermercati, dall'altra alcune informazioni che accompagnano il codice a barre che identifica la tessera.
Nessuna banda magnetica, nessuna possibilità di leggerla e craccarla, o modificare dei dati che vi sono memorizzati. Un pezzo di plastica, insomma, che potrebbe essere la mia, potrebbe essere la vostra e quella di chiunque. Ne siamo certi? Lo vedremo.

:: La realtà svelata

Cominciamo col dire che, quando abbiamo deciso di farci la tessera, abbiamo parlato con una signorina alla reception che con un grande sorriso ci ha porto un modulo da compilare e una penna. Su questo modulo abbiamo dovuto scrivere tutti i nostri dati personali: la tessera non è quindi così anonima come credevamo. Il regolamento lo dice chiaro: la tessera è personale e non cedibile, e i dati nel modulo devono essere veritieri pena l'impossibilità a rilasciarla o al ritiro della stessa. A quel codice a barre, quindi, corrispondono il nostro nome e indirizzo: chi vi ha accesso saprà che cosa abbiamo comprato dal momento in cui abbiamo sottoscritto il modulo. Cosa significa in parole povere? Significa che osservando la frequenza con cui compro una scatola di preservativi qualcuno saprà quante volte faccio l'amore con la mia fidanzata, osservando i miei acquisti di carta igienica... Dati statistici che, cumulati con quelli di altre persone, guideranno l'azienda nelle azioni future (per non parlare della pubblicità mirata).

::Dulcis in fundo: i premi

Studiamo un momento ora gli sconti promessi per i possessori della tessera. Sono davvero così vantaggiosi? All'apparenza può sembrare, anche se non sono mai significanti uno può essere portato a pensare che sommandoli tutti in una spesa qualcosa facciano. Forse si. Ma guardiamo cosa abbiamo nel carrello: c'è solo ed esclusivamente ciò per cui siamo entrati nel supermercato? Sono pronto a scommettere che nove volte su dieci abbiamo preso dagli scaffali altri prodotti che non erano nella nostra lista. Costo prodotti aggiunti senza necessità meno sconto della tessera dà comunque un saldo a favore del punto vendita.

Infine la nota dolente: i premi. Sfoglio il catalogo e vedo che un bel lettore MP4 di marca posso averlo gratis con 8300 punti. Il regolamento della tessera dice che ho diritto a due punti ogni euro di spesa a partire dai cinque euro: volendo farne 8300 in una sola spesa dovrei comprare prodotti per 4155 euro. Improponibile. Lo faccio in più spese successive? È così che normalmente funziona, ma per ogni spesa dovremmo aggiungere i cinque euro iniziali. Ammettendo di fare una spesa media mensile di 400 euro e di spendere 100 euro a settimana, raggiungeremmo la quota in "solo" 44 settimane e 4400 euro di spesa. 245 euro in più. Il prezzo di listino del lettore è di 100 euro... Sul Web lo si trova intorno ai 95 euro, ma questo vale per oggi: tra quasi un anno, quando avremo abbastanza punti, lo stesso lettore costerà almeno un buon 20% in meno. Se contiamo che almeno il 20% di quei 4400 euro è costituito da prodotti di cui non avevamo bisogno e che probabilmente finiranno in spazzatura... ne vale la pena?

Recupero totale

Se si rompe un disco di un RAID recuperare i dati è facile. Se si rompe il controller, le cose si complicano.

Possiamo definire un RAID come un insieme di dischi fisici che si comportano come un unico disco logico. I motivi per cui utilizzare un sistema RAID sono i più diversi: aumentare l'affidabilità del computer, aumentare la velocità di lettura o scrittura del disco, unire tra loro più dischi di piccole dimensioni in un disco logico più grande e così via. A ognuna di queste geometrie equivale un livello standard di RAID che parte da zero, nel caso di due o più dischi uniti a formarne uno unico e senza ridondanza, e arriva al sette, dove sono presenti più dischi con sistemi di tolleranza alla rottura di uno o più dischi e una cache in lettura che ne migliora le prestazioni.

Solitamente, quando vogliamo avere la garanzia che la rottura di un disco, ricorriamo a un RAID di livello 5 oppure, in casi minori, a un RAID di livello 4 o 6. Altre volte la ridondanza è ottenuta applicando più livelli di RAID contemporaneamente, come nel caso dei RAID 1+0 e 0+1 e sacrificando interi dischi per tenere in mirror le unità, aumentando le possibilità di recupero.

:: Punto debole

In realtà, qualsiasi geometria ha un punto debole: il controller RAID e le diverse implementazioni che i vari costruttori realizzano. Partendo dallo stesso approccio teorico, infatti, molti costruttori realizzano sistemi RAID equivalenti che, tuttavia, hanno modalità diverse di dividere i dati tra i dischi. Con l'eccezione dei semplici mirror, RAID 1, togliendo i dischi RAID da un sistema e mettendoli su un altro, di un altro costruttore, il RAID non risulta più funzionante. In alcuni casi, addirittura, non è più nemmeno possibile ricostruirlo usando le utility standard. In ambito server, dove i RAID sono diffusi da sempre, questi casi sono del tutto marginali: è rarissimo che la rottura di un controller RAID dia questi problemi. Quasi sempre, il controller RAID non è altro che una piccola scheda aggiunta alla motherboard che viene, semplicemente, sostituita con una identica e non può avere problemi di questo tipo.

Con la diffusione in ambito casalingo dei RAID questa situazione non si presenta: l'inclusione del controller RAID nelle schede madri, il continuo ricambio tecnologico, l'uscita di schede madri sempre migliori, la presenza sul mercato di innumerevoli concorrenti, rendono piuttosto difficile riuscire a recuperare un RAID nel caso in cui ci siano problemi alla scheda madre con cui è stato creato. Se, in linea teorica, basterebbe cambiare la motherboard danneggiata con una identica, il recupero di una motherboard identica, persino dello stesso costruttore, è spesso un'impresa disperata. Così si viene a creare una situazione paradossale per cui la rottura di

qualche componente elettronico della scheda madre impedisce l'accesso a un RAID in cui i dati sono integri e la sua sostituzione con una motherboard simile, ma con un'implementazione anche solo parzialmente diversa del RAID, non permette l'accesso ai dati. In tutti questi casi è possibile rassegnarsi e formattare i dischi, perdendone il contenuto, oppure provare a un tentativo di ricostruzione del RAID tramite strumenti terzi.

:: Ridammi i dati!

Uno degli strumenti software più affidabili che permettono il recupero dei dati anche agli utenti inesperti si chiama GetDataBack ed è prodotto in due versioni, per FAT e per NTFS, dalla Runtime Software, www.runtime.org. Il suo funzionamento si basa su un'analisi completa della superficie dei dischi interessati ignorando totalmente le funzioni del controller a cui sono collegati. La ricostruzione che viene fatta, quindi, è logica e prescinde sia dal tipo di RAID originario che dal controller a cui i dischi sono attualmente collegati. Questo significa che potremmo prendere 2 dischi in RAID 0, collegarli a un controller che non ha alcuna funzione RAID e ricostruire il disco logico equivalente, anche se al sistema operativo sembreranno dischi vuoti. Altra caratteristica di GetDataBack è quella di poter ignorare qualsiasi informazione di sistema sui file ma di affidarsi solo ai dati fisicamente scritti: ideale per il recupero di dati eliminati accidentalmente.

Il funzionamento del programma è molto semplice ma non bisogna lasciarsi ingannare: andando oltre le impostazioni di base, il programma diventa uno strumento potentissimo di recupero dei dati.

RAID 1-0 sono i più diffusi in ambito server: uniscono la velocità e la capacità del RAID 0 con la sicurezza e le possibilità di recupero dati tipiche del RAID 1.

Per prima cosa ci viene chiesto di indicare il problema che vogliamo risolvere: recupero di file cancellati, errate formattazioni, distruzione estesa dei dati come avviene nel caso di re installazione di un sistema operativo e così via. Nel dubbio possiamo lasciare le impostazioni di default, che svolgono tutte le analisi in modo approfondito, anche se il tempo richiesto si allungherà notevolmente. Nel passo successivo dovremo selezionare i dischi interessati dal problema. Nel caso di un RAID con più dischi, non preoccupiamoci troppo dell'ordine in cui li selezioniamo: il programma li analizza e riconosce da solo la struttura RAID utilizzata.

Il passo successivo è proprio l'analisi dei dischi e l'identificazione dei file system presenti: GetDataBack ci fornirà una lista dei possibili file system da recuperare e delle loro caratteristiche e noi potremo scegliere quello che pensiamo sia il più corretto. Una volta fatta questa scelta, ci verrà mostrata una finestra simile a quella di Internet Explorer con l'elenco dei file e delle cartelle presenti sul disco e alcune indicazioni delle caratteristiche dei dati: nascosti, cancellati, compressi e così via. Da questa finestra avremo la possibilità di recuperarli tutti o in parte, semplicemente copiandoli su un altro disco, anche di rete. GetDataBack funziona in modo così lineare che l'operazione che compie potrebbe quasi sembrare banale ma non lasciamoci ingannare: in alcune situazioni, l'analisi che viene fatta sui dischi è molto complessa, così come il tempo può essere notevole: anche 1 ora per ogni Gb da recuperare.

IL SISTEMA RAID

Esistono molte implementazioni di sistemi RAID ma quelle più diffuse sono 5: RAID 0, JBOD, RAID 1, RAID 5, RAID 10.

Nel **RAID 0**, due o più dischi sono uniti tra loro in un'unica unità logica e i dati sono spezzati in blocchi che vengono scritti su tutti i dischi. Se pensiamo a un file composto da blocchi e un RAID 0 composto da due dischi, la situazione tipica è che viene scritto il blocco 1 sul disco 1, il blocco 2 sul disco 2, il blocco 3 sul disco 1 e così via. Il vantaggio immediato è la velocità di scrittura e la riduzione dei dischi logici nel sistema ma la sua affidabilità è inversamente proporzionale al numero di dischi coinvolti nel RAID. Simile al RAID 0, il **JBOD** prevede la concatenazione di più dischi in un'unica unità logica. La velocità di lettura e scrittura non varia rispetto alle caratteristiche fisiche dei dischi che lo compongono ma in caso di guasto a un disco, la perdita è limitata ai dati che contiene e non all'intero disco logico.

Il **RAID 1** è chiamato anche mirror e prevede che due o più dischi vengano scritti contemporaneamente con gli stessi dati. Lo svantaggio è la perdita di spazio ma ha il grande vantaggio che la rottura di un disco non influisce sul sistema.

Diversamente dai sistemi visti fin'ora, il **RAID 5** richiede almeno 3 dischi per funzionare. I dati vengono scritti su due dischi come avviene per il RAID 0 mentre su un terzo disco vengono scritte informazioni di parità. In questo modo, grazie al controllo di parità è possibile ricostruire i dati persi a causa di un eventuale disco rotto.

Il **RAID 10** è, in realtà, una combinazione di RAID 1 e di RAID 0 e richiede almeno 4 dischi: questi sono collegati a due a due in RAID 1 e i blocchi, tra loro, in RAID 0.

Implementazione OCR e reti neurali in JavaScript

COME BUCARE UN CAPTCHA

Odiosi, efficaci, a volte troppo poco leggibili... ormai siamo abituati a dover inserire delle lettere o numeri rappresentati graficamente, per verificare che non sia un software che sta accedendo in automatico a quella pagina web.
Una misura creduta abbastanza efficace per contrastare lo spam e gli abusi, finché non si è saputo che ormai esistono delle spam-farm, dei centri di produzione di spam dove per pochi centesimi lavorano degli "schiavi" (cliteratureblog.blogspot.com/2009/01/captcha-slave-labor.html) che devono riconoscere e superare manualmente queste difese che prendono il nome di CAPTCHA.

In altri casi, il CAPTCHA viene utilizzato per impedire una fruizione semplice di un servizio gratuito, allo scopo di promuovere la versione a pagamento. È il caso di Megaupload, il famoso spazio web che permette di caricare online file pesanti che possono essere poi scaricati agevolmente da chiunque conoscendo il link di riferimento.

Una volta aperto tale link però, per poter scaricare il file va inserito un codice CAPTCHA composto da 3 lettere, dopodiché viene avviato un timer (variabile in base alla quantità di scaricamenti che ha già subito il file) prima che il download sia effettivamente reso disponibile.

È già abbastanza noioso dover attendere, ma si deve anche andare a leggere la pagina appena aperta per poter inserire il CAPTCHA o l'attesa non avrà fine. Non sarebbe comodo avere un software che inserisce il CAPTCHA al posto nostro e che magari si preoccupa di scaricare anche il file quando il timer è scaduto?

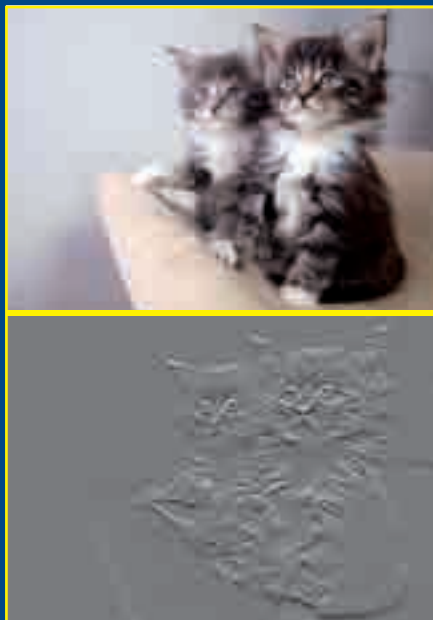
:: Aggiriamoli

Grazie a del codice JavaScript e uno script per GreaseMonkey (famoso plugin per Firefox), scritti da Shaun Friedle, è possibile superare automaticamente i blocchi CAPTCHA di Megaupload.

GWL MWQ TDD

Alcuni CAPTCHA che vengono automaticamente riconosciuti.

Effettivamente la protezione non è molto complessa, ma è davvero molto interessante la soluzione che Shaun ha implementato. Shaun ha utilizzato una API Canvas chiamata getImageData implementata nel draft HTML 5 che permette di selezionare e processare le immagini online allo stesso livello dei programmi di fotoritocco (www.whatwg.org/specs/web-apps/current-work/#dom-context-2d-getimagedata). Ha poi implementato una rete neurale scritta completamente in Javascript che è stata allenata a riconoscere i CAPTCHA di Megaupload attraverso i pixel estratti dal Canvas, realizzando in qualche modo un OCR grezzo ma molto efficace.

Avendo come obiettivo quello di riconoscere un CAPTCHA di sole tre lettere scritte in modo abbastanza chiaro era prevedibile che il codice non fosse troppo complesso, ma stiamo comunque parlando di reti neurali. Ognuna delle lettere del CAPTCHA è colorata diversamente, è scelta da un alfabeto di 26 simboli, ma è rappresentata nello stesso font. Quindi come primo step il CAPTCHA viene copiato tramite canvas e convertito in toni di grigio. Successivamente l'immagine viene separata in tre matrici (ognuna delle quali contiene solo uno dei caratteri identificato dal diverso tono di grigio rispetto agli altri) e tramite un semplice filtro basato sui pixel circondati da un diverso colore viene rimosso il rumore eventualmente presente.

La procedura si basa sul principio di questa trasformazione grafica.

L'ultimo passo prima di passare il simbolo alla rete neurale consiste nel definire meglio il perimetro del simbolo, ossia la sua forma. Viene identificato il rettangolo minimo contenente il simbolo che viene scalato in una matrice di 20x25 pixel e reso monocolore. Poi vengono applicate alcune finezze: il rettangolo viene ulteriormente ridotto e un numero di pixel "strategici" vengono estratti per fungere da recettori che alimentano la rete neurale (resa necessaria dall'elevato livello di ambiguità che comunque si realizza con i filtraggi e le scalature applicati).

:: Fase finale

Ora l'algoritmo è pronto per indovinare la lettera. La rete neurale è stata alimentata con 64 input booleani scelti da una delle lettere estratte, oltre ad avere una serie di valori precalcolati (uno dei concetti chiave delle reti neurali è che la rete va allenata con dei risultati significativi ottenuti da prove precedenti) e procederà quindi a confrontare il simbolo con tutto l'alfabeto inglese, assegnando per ciascuna lettera una percentuale di similitudine. Non si otterrà mai un 100%, ma è probabile che l'algoritmo raggiunga anche un 98% di similitudine e il tutto utilizzando una tecnologia standard del browser! Per godersi lo spettacolo è sufficiente installare GreaseMonkey e aggiungere un nuovo script in cui copiare l'ultima revisione del codice di Shaun (userscripts.org/scripts/show/38736).

Abilitando lo script ad attivarsi per Megaupload.com e aprendo uno dei link per scaricare un file, vedremo lavorare l'algoritmo: comparirà un "working" che sarà successivamente sostituito dalle lettere riconosciute, dopodiché si avvierà il contatore per il download. Purtroppo nelle prove che ho fatto con l'ultima rev. 0.0.5 il download non parte quando il timer arriva a zero ma aprendo la finestra in background ce la troveremo comunque con il link pronto a partire! Per superare anche quest'ultimo scoglio basta installare un altro script per GreaseMonkey, Megaupload Helper (userscripts.org/scripts/show/6764) e il download partirà da solo alla fine del timer.

(Il cuore dell'algoritmo)

```
function get_code(image)
{
  var canvas = unsafeWindow.document.createElement("canvas");
  canvas.width = image.width;
  canvas.height = image.height;
  canvas.getContext("2d").drawImage(image, 0, 0);
```

TUTTI AL FRONTE

Polemiche e proteste per una proposta di legge che sembra dettata dalla SIAE e colpisce tutti gli utenti e gli operatori di Internet.

Dura lex, sed lex, dicevano gli antichi romani, ovvero: dura legge ma legge. Probabilmente perché vivevano in mondo certamente meno complesso di quello di oggi e avevano legislatori che sapevano su cosa stavano legiferando. Lo stesso, purtroppo, non accade da noi: dopo Nicolas Sarkozy, presidente francese, che ha dichiarato una vera e propria guerra al peer-to-peer minacciando la disconnessione di chi condivide materiale protetto dal diritto d'autore, anche il parlamento italiano cerca di adeguarsi a quella che, a livello mondiale, è ritenuta una dottrina fallimentare. Al Comitato Governativo è arrivata una proposta di legge che illustra alcune *"disposizioni concernenti la diffusione telematica delle opere di ingegno"* che, in 25 righe, dà carta bianca al governo di agire, tramite regolamenti tecnici e decreti su misura, contro utenti e *"prestatori di servizi della società dell'informazione"*. Quest'ultima definizione dice tutto e non dice nulla perché chiunque abbia a che fare con Internet, ma non solo, può essere definito in questo modo: da chi scrive un blog a chi risponde a un messaggio in una chat, da YouTube a Google.

Il documento PDF diffuso sul Web con il testo della proposta di legge: la SIAE ne nega la paternità ma le informazioni al suo interno dicono il contrario.

:: Arriva la censura

Proprio il coinvolgimento dei provider nella definizione della proposta la fa partire con il piede sbagliato:

in nome della neutralità della rete e del fatto che la connettività è vista in sede europea come un bene primario, lo stesso parlamento europeo ha bocciato più volte, in passato, leggi simili. Lo stesso problema ce l'ha attualmente il presidente francese Nicolas Sarkozy, novello paladino delle società dei diritti d'autore: il suo tentativo di far varare una legge che preveda la disconnessione degli utenti che scaricano file illegalmente è stato bocciato con larga maggioranza in sede europea. Non va meglio con altri aspetti della proposta, in particolare quando chiede ***"l'attribuzione di poteri di controllo alle Autorità di Governo ed alle Forze dell'ordine per la salvaguardia su tali piattaforme telematiche del rispetto di norme imperative, dell'ordine pubblico, del buon costume, ivi inclusa la tutela dei minori"***. In pratica, la proposta di legge inneggia alla creazione di strumenti che permettano alle Autorità di controllare i contenuti pubblicati dagli utenti.

Altroconsumo, www.altroconsumo.it, è stata la prima associazione di consumatori a rendere nota questa proposta di legge così contestata.

European Parliament votes against 3-strikes

Tutti i siti che si occupano di notizie riguardanti Internet hanno dato ampio risalto alla clamorosa bocciatura della dottrina Sarkozy

Un differenza lieve ma fondamentale con l'attuale persecuzione di reati compiuti attraverso Internet, per la quale esistono già gli strumenti adatti. La definizione inserita in questa proposta, invece, permetterebbe alle Forze dell'Ordine di cancellare post scomodi dei blog, eliminare notizie non approvate ufficialmente, eliminare qualsiasi genere di video e via dicendo. In un ambiente come Internet, in cui è molto complesso dimostrare legalmente la cancellazione di materiale, questi provvedimenti non permetterebbero alcuna tutela degli utenti dall'arbitrio di chi deve controllarli. Non che questo paragrafo della proposta di legge sia una norma inventata dai proponenti: da anni viene applicata una norma simile, con ottimi risultati, in Cina. Allo stato attuale, questa è solo una proposta di legge che, del tutto casualmente, vede l'opposizione di esperti, utenti e fornitori di servizi mentre viene accolta con calore da FIMI e SIAE, ormai disposte a tutto per tornare agli antichi fasti dopo aver fallito il tentativo di adeguarsi alle nuove tecnologie. Proprio la possibilità di introduzione della censura, ricorrente quando si tratta di limitare la libertà di espressione con un mezzo poliedrico come Internet, ha dato non pochi problemi persino per tutelare i minori dallo sfruttamento e dalla pornografia: il Child Safe Act, proposto da Bush e nobilissimo negli intenti, è stato bocciato perché lesivo delle libertà minime garantite dalla Costituzione americana.

:: Inapplicabile

Dal punto di vista pratico, inoltre, se la proposta dovesse diventare legge si presenterebbe una situazione, purtroppo, già vista: l'inapplicabilità assoluta. L'incarico di controllare il materiale presente in Rete verrebbe affidato alle Forze dell'Ordine che sono già sovraccariche di compiti e che hanno già difficoltà a perseguire reati odiosi come la pedofilia o reati dannosi per lo Stato intero come la truffa o il gioco d'azzardo illegale. Inoltre non viene fatta, come sempre quando si tratta di Internet, alcuna considerazione del fatto che si sta parlando di un contesto internazionale in cui le leggi italiane non hanno alcun valore.

L'azione dei magistrati che volessero perseguire un post su un blog ospitato da un server negli USA, tanto per fare un esempio, dovrebbe essere compiuta tramite una rogatoria internazionale, scontrandosi con una legislazione diversa che tutela quel post come libera espressione. Come ciliegina sulla torta c'è anche la considerazione che l'identificazione di chi mette online materiale di qualsiasi genere è quantomeno complessa: richiede tempo, richiede la prova che non il computer ma la persona abbia compiuto determinate azioni e viene vanificata dal fatto che non è necessario usare la propria connessione per compiere un reato ma più frequentemente si usano connessioni rubate da altri oppure connessioni aziendali. Proprio su questo punto, inoltre, una legislazione con un orientamento alla Sarkozy potrebbe fare danni gravissimi: sarebbe un disastro che la pubblicazione reiterata di materiale fuorilegge proveniente da reti aziendali portasse alla disconnessione dell'azienda.

Misteri svelati

Analisi di protocolli sconosciuti: come si fa e cosa possiamo scoprire

Le trasmissioni su una rete viaggiano per mezzo di pacchetti di dati determinati dai protocolli utilizzati dal software. Questi protocolli codificano le informazioni in maniera che siano riconoscibili dal computer di destinazione e dal software che vi è in esecuzione. Finché si tratta di un protocollo documentato non sussiste alcun problema, troviamo molte informazioni sulla sua implementazione. Ma nulla vieta a un produttore software di crearsi un protocollo proprietario e di usare quello per le sue trasmissioni, senza divulgare alcunché sul suo funzionamento. In questo caso, capire come funziona può diventare un lavoro da veri certosini informatici.

:: Strumenti di analisi

Per prima cosa ci serve un buon packet sniffer in grado di fare il dump dei dati che passano attraverso il cavo di rete. Qui usiamo Wireshark, che è gratuito e si può scaricare liberamente da www.wireshark.org; inoltre, questo programma compie in autonomia una certa parte del lavoro, identificando per noi i pacchetti dei protocolli riconoscibili. Questi ultimi ci sono molto utili come "palestra", per allenare l'occhio alla struttura dei protocolli e a individuare in fretta quelli che possono essere dati salienti, come stringhe, timestamp o indirizzi di rete, che nei protocolli non riconoscibili possono essere presenti ma individuabili solo con un po' di pratica.

Un altro strumento molto utile è un programma che possa fare un confronto tra due file e segnalare visivamente le differenze eventualmente riscontrate. È preferibile un programma che permetta di analizzare i file in forma binaria (cioè con il loro contenuto in valori esadecimali), come il programma freeware AptDiff (http://www.aptedit.com/aptdiff.htm). In questo modo potremo comparare due pacchetti catturati in tempi diversi per evidenziarne le differenze e in-

Una sessione di cattura del traffico di rete con Wireshark in versione per Windows.

dividuarle a colpo d'occhio. Infine, armiamoci di cervello, qualcosa da bere (o da sgranocchiare) e tanta, tanta pazienza, ci serviranno molto.

:: Hands on

Prendiamo in esame qualcosa di conosciuto e di facile interpretazione, ma che ci può essere d'aiuto per fare esperienza e riconoscere quindi pattern che possono ripresentarsi in altre situazioni. Non abbiamo scelto a caso Wireshark: con la sua interfaccia possiamo individuare facilmente i singoli elementi che compongono il pacchetto in esame. Avviamolo e iniziamo a catturare il traffico di rete. La schermata principale si popolerà immediatamente con l'elenco dei pacchetti ricevuti.

La vista sarà un po' monotona se in rete abbiamo acceso solo un computer, ma con diversi computer la cosa cambia. È sufficiente qualche secondo, poi possiamo fermare la capture e iniziare la nostra analisi. Vediamo subito che sono presenti numerosi pacchetti NBNS: si tratta del protocollo NetBIOS di Microsoft, usato per le comunicazioni di rete in ambiente Windows. Un'ottima palestra per i nostri scopi, a patto che facciamo finta di non conoscerlo. Salviamo quindi qualche pacchetto NBNS in file separati e iniziamo la nostra analisi.
Avviamo AptDiff, indichiamo i primi due pacchetti e ricordiamoci di specificare che vogliamo confrontarli come file binari. La vista della finestra principale possiamo organizzarla a piacere, affiancando i due file in verticale o in orizzontale, l'importante è che possiamo leggere con chiarezza i valori mostrati. Nel nostro caso, notiamo subito che si differenziano lievemente l'uno dall'altro, e questa è una cosa che facilita l'analisi nel caso ci trovassimo davanti a un protocollo sconosciuto: una sola capture non ci direbbe molto, mentre due sovrapposte per lo meno ci indicano le variazioni nel tempo. Saltiamo i primi 40 byte che fanno parte del formato di file di Winpcap (la libreria di cattura usata da Wireshark) e notiamo che ci sono due sequenze di sei byte separate da uno zero: niente di più facile che si tratti di indirizzi MAC che identificano i computer sulla rete. In particolare, la prima sequenza tutta composta da valori pari a 255 (0xFF in esadecimale) fa pensare a una trasmissione di tipo broadcast.
Il primo byte che cambia è alla posizione 0x3B: 4C nel primo pacchetto, 4D nel secondo pacchetto. Questo fa presumere a un counter di qualche tipo; un'analisi successiva tra il secondo e il terzo pacchetto catturato potrebbe darcene la conferma o la smentita. Sorge quindi un dubbio: cosa succede quando il byte arriva al massimo valore consentito? Riparte semplicemente da zero o avviene una variazione anche dei byte contigui, indicando quindi che il counter non si limita a 256 valori compreso lo zero ma misura valori ben più grandi. Più avanti troviamo una lunga stringa di caratteri alfabetici, che potrebbe trattarsi dei dati effettivamente trasmessi dal pacchetto.

Il confronto con AptDiff di due dei pacchetti salvati in precedenza.

La verifica con Wireshark: se le nostre supposizioni erano esatte, studiando il pacchetto NetBIOS nell'applicazione ne avremo conferma.

:: La verifica

Se torniamo a esaminare i pacchetti in Wireshark, che naturalmente li riconosce perfettamente come pacchetti NetBIOS, possiamo scoprire che non ci siamo allontanati di molto dalla realtà. Effettivamente le due sequenze di sei byte si riferiscono rispettivamente a tutta la rete (quindi broadcast) e all'indirizzo MAC della fonte, cioè del computer che ha trasmesso il pacchetto. Scopriamo anche che il presunto counter in effetti identifica il pacchetto IP trasmesso con un numero sequenziale, e che la lunga stringa di caratteri alfabetici non è altro che la codifica del nome NetBEUI del computer sorgente. Oltre alla cattura dei pacchetti, se siamo in possesso dell'applicazione che li genera possiamo anche tentare di disassemblarla e studiarne il comportamento in rete, e questo renderebbe più facile riconoscere i valori inseriti in uno specifico datagramma Ethernet.

Come funziona un attacco al sistema di smistamento dei pacchetti di una LAN per intercettare le comunicazioni

L'UOMO IN MEZZO CI ASCOLTA

Stiamo parlando del tipico attacco "Man In The Middle", sfruttato sin dal principio per intercettare le comunicazioni che passano attraverso i cavi di rete e che fa affidamento su una debolezza intrinseca del sistema, ossia il fatto che i pacchetti ARP non necessitano di autenticazione e possono quindi essere facilmente falsificati.
Con questa tecnica è possibile semplicemente "ascoltare" ciò che due computer si dicono (arrivando a leggere le password in chiaro che alcuni protocolli trasmettono) oppure causare interruzione dei servizi con il più tipico degli attacchi DoS.

:: Come funziona ARP

ARP sta per Address Resolution Protocol e serve per mappare, in una rete locale, l'indirizzo IP di un computer con l'indirizzo MAC della sua scheda di rete. Questo funzionamento è utile su una rete commutata perché il sistema deve sapere a quale macchina inoltrare un pacchetto, pertanto chiede alla LAN qualcosa del tipo "a quale indirizzo MAC corrisponde l'IP x.x.x.x?" e, una volta ricevuta la risposta, la memorizza in una cache e da quel momento continuerà a inviare i pacchetti con destinazione IP x.x.x.x all'indirizzo MAC ottenuto con l'interrogazione. È un po' il funzionamento del DNS su Internet: per raggiungere un sito, scriviamo il suo indirizzo mnemonico nel browser e il server DNS lo traduce nell'indirizzo IP del server Web su cui risiede.
In **Figura 1** vediamo un semplice esempio di questo funzionamento: l'host 192.168.1.102 vuole pingare

No.	Time	Source	Destination	Protocol	Info
725	355.536520	192.168.1.10	235.1.1.1	IGMP	V2 Membership Report / Join group 235.1.1.1
726	355.560979	192.168.1.1	224.0.0.1	IGMP	V2 Membership Query, general
727	356.800993	AsustekC_08:7e:92	Broadcast	ARP	Who has 192.168.1.107? Tell 192.168.1.102
728	356.801530	SamsungE_2f:85:48	AsustekC_08:7e:92	ARP	192.168.1.107 is at 00:15:99:2f:85:48
729	356.801536	192.168.1.102	192.168.1.107	ICMP	Echo (ping) request
730	356.801951	192.168.1.107	192.168.1.102	ICMP	Echo (ping) reply
731	357.788681	192.168.1.102	192.168.1.107	ICMP	Echo (ping) request
732	357.789330	192.168.1.107	192.168.1.102	ICMP	Echo (ping) reply
733	358.194734	192.168.1.102	224.0.0.251	IGMP	V2 Membership Report / Join group 224.0.0.251
734	358.788709	192.168.1.102	192.168.1.107	ICMP	Echo (ping) request

***Figura 1** - Un semplice ping verso un host della rete ha generato anche la richiesta ARP per individuarne l'indirizzo MAC.*

l'host 192.168.1.107, viene generata una richiesta ARP che chiede alla rete chi ha l'indirizzo 192.168.1.107 (riga 727), quest'ultimo risponde direttamente con "ho io 192.168.1.107 e il mio MAC è 00:15:99:2F:85:48" (riga 728); dopodiché avviene la trasmissione dei pacchetti ICMP del comando ping, con relative risposte (righe da 129 in avanti).

:: Struttura di un pacchetto ARP

La struttura di un pacchetto ARP è definita secondo il frammento di Codice 1, tratto dal file if_arp.h nei sorgenti Linux.

```
[Codice 1]
struct  arphdr {
        u_short ar_hrd;         /* Format of hardware address */
        u_short ar_pro;         /* Format of protocol address */
        u_char  ar_hln;         /* Length of hardware address */
        u_char  ar_pln;         /* Length of protocol address */
        u_short ar_op;          /* one of: */
#define ARPOP_REQUEST   1       /* Request to resolve address */
#define ARPOP_REPLY     2       /* Response to previous request */
#define ARPOP_REVREQUEST 3      /* Request protocol address given hardware */
#define ARPOP_REVREPLY  4       /* Response giving protocol address */
#define ARPOP_INVREQUEST 8      /* Request to identify peer */
#define ARPOP_INVREPLY  9       /* Response identifying peer */
#ifdef COMMENT_ONLY
        u_char  ar_sha[];       /* Sender hardware address */
        u_char  ar_spa[];       /* Sender IP address */
        u_char  ar_tha[];       /* Target hardware address */
        u_char  ar_tpa[];       /* Target IP address */
#endif
};
```

:: Sfruttare ARP Reply

Premettiamo che ARP non è solamente un protocollo che serve per associare indirizzi IP e indirizzi MAC, ma bensì un protocollo generico che ha anche altri utilizzi. In questo caso però ci interessa il semplice uso IP.
Osservando la struttura, possiamo sapere che il campo ar_op viene usato per inviare il vero e proprio comando ARP, per esempio ARPOP_REQUEST o ARPOP_REPLY che identificano il tipo di pacchetto (richiesta o risposta). Sono interessanti anche Sender hardware address, Target hardware address e Target IP address, che immagazzinano nell'ordine: indirizzo MAC dell'host che compie la richiesta, indirizzo MAC dell'host che risponde e indirizzo IP di quest'ultimo.
Sender hardware e Sender IP indicano sempre gli indirizzi MAC e IP di chi fa la richiesta, mentre gli indirizzi del Target cambiano secondo il caso. Quando si compie una richiesta, l'indirizzo Target hardware viene riempito da zeri perché non lo si conosce, mentre Target IP contiene l'IP di destinazione.

Nel momento in cui l'host di destinazione risponde, si occupa solo di inserire il proprio MAC al posto degli zeri e di cambiare ar_op da ARPOP_REQUEST a ARPOP_REPLY e reinvia il pacchetto indietro al Sender, ovviamente invertendo gli indirizzi Sender che ora indicano se stesso con gli indirizzi Target, a questo punto riferiti all'host che ha effettuato la richiesta originale. Ora il Sender iniziale aggiorna la propria cache ARP con le informazioni ricevute e, fino alla scadenza di queste ultime, anche le informazioni della cache ARP hanno la propria TTL (Time To Live) come i pacchetti TCP o i dati DNS, non compierà ulteriori richieste per conoscere l'indirizzo MAC di Target e continuerà la comunicazione prelevando l'indirizzo dalla propria cache. In Figura 2 vediamo in dettaglio la richiesta ARP, mentre in Figura 3 troviamo la relativa risposta.

:: L'attacco

Ma cosa succede se tra il Sender e il Target si inserisce qualcuno che falsifica il contenuto dei pacchetti ARP di risposta, sostituendo il MAC address di Target con il proprio?
È facile da intuire: Sender aggiornerà la propria cache con l'indiriz-

```
= Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: AsustekC_08:7e:92 (00:0e:a6:08:7e:92)
    Sender IP address: 192.168.1.102 (192.168.1.102)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.107 (192.168.1.107)
```

***Figura 2** - I dettaglio della richiesta ARP: notiamo lo spazio dedicato al Target MAC impostato a zero, che verrà riempito dal Target con la risposta.*

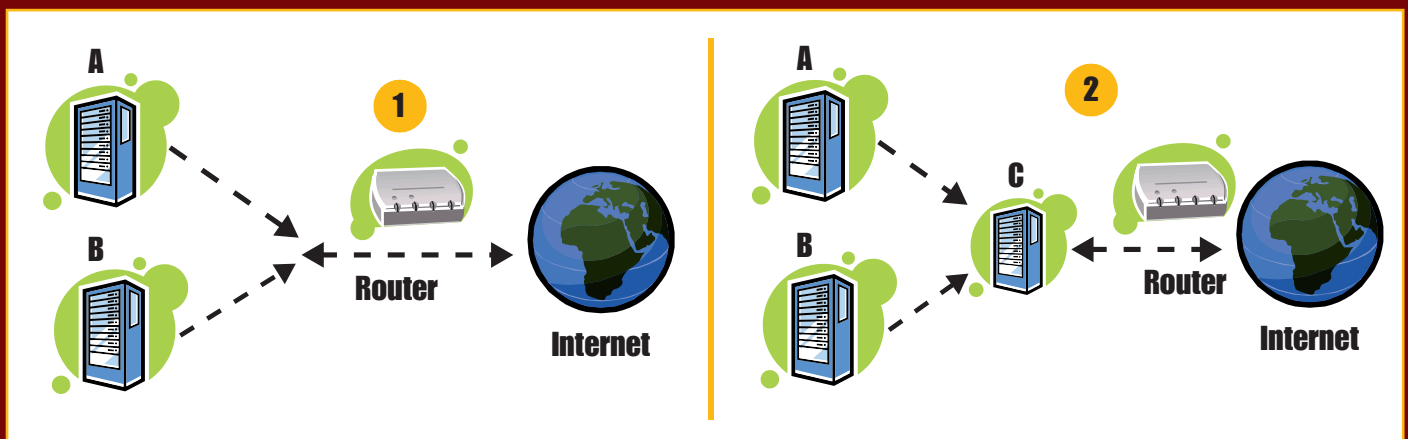
zo sbagliato e tutte le comunicazioni future le dirotterà verso l'intruso, il quale potrà instradarle alla corretta destinazione per rendere trasparente il passaggio e, nel frattempo, analizzare il contenuto dei pacchetti. Il classico Man In The Middle, per intenderci. Vediamo come funziona.
Usando un software per effettuare packet injection, l'attaccante cerca di indurre la vittima a creare un'entry nella propria cache ARP usando un IP inesistente, iniettando false richieste ARP usando come Sender IP quello fasullo e come Sender Hardware il proprio reale. Usando come destinazione FF:FF:FF:FF:FF:FF (cioè tutta la rete) non si ottiene risposta, ma indirizzando le richieste direttamente all'host vittima questo crea la voce nella cache e risponde adeguatamente. Da quel momento tutte le comunicazioni di rete della vittima vengono ricevute anche dal computer dell'attaccante, il quale non fa altro che catturarle per poterle salvare e reinstradarle in rete per agire in maniera trasparente.

```
= Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: SamsungE_2f:85:48 (00:15:99:2f:85:48)
    Sender IP address: 192.168.1.107 (192.168.1.107)
    Target MAC address: AsustekC_08:7e:92 (00:0e:a6:08:7e:92)
    Target IP address: 192.168.1.102 (192.168.1.102)
```

***Figura 3** - Stesso dettaglio per quanto riguarda la risposta del Target: gli indirizzi Target e Sender sono invertiti e il comando ar_op trasformato in Reply.*

:: Come difendersi

Tutto ciò è possibile perché il protocollo ARP, come già detto, non richiede alcuna autenticazione e quindi i computer "si fidano" di ciò che ricevono.

Per potersi difendere da questo tipo di attacco si può per esempio adottare IPv6, IPsec oppure adottare tabelle ARP statiche. Se abbiamo modo di monitorare le comunicazioni di rete, usando un pacchetto come arpwatch abbiamo modo di individuare subito comportamenti anomali e prendere le adeguate contromisure. In alternativa, si può adottare anche SARP, cioè Secure ARP, un'estensione di questo protocollo in grado di autenticare il Sender, oppure implementare il port security degli switch di rete, che forza la corrispondenza di ogni porta del dispositivo con un singolo indirizzo MAC. La soluzione migliore però è implementare una rete 802.1x con server RADIUS che forza l'autenticazione remota. Comunque è bene stare sempre all'erta: sniffare il traffico della propria rete ogni tanto, per sicurezza, non guasta mai.

Nello Schema 1 il flusso di una comunicazione normale; in Schema 2 invece il classico attacco di tipo "Man in the Middle": il computer C, quello dell'Hacker, intercetta la comunicazione tra le macchine A e B fingendo di essere un PC autorizzato della rete.

CREA IL TUO SITO DI HACKER JOURNAL

CE LA FAI CON L'FBI

L'ufficio investigativo federale americano pubblica in rete cifrari fin troppo facili. Perché?

Viene da chiedersi perché l'Fbi dovrebbe mettersi a pubblicare cifrari su Internet. Oltretutto, specie per noi di Hacker Journal, dovrebbe essere materiale molto semplice. Ricordiamoci che è tutto scritto in inglese e guardiamo il primo cifrario: quella sequenza YYY.AHB.MSK/ non potrebbe ricordare qualcosa? Per esempio l'inizio di un sito? www... si può partire dall'ipotesi che Y sia una codifica di W e che la sequenza inizi con WWW. Se davvero è l'indirizzo di un sito, potrebbe essere il sito dell'Fbi. Il sito dell'Fbi è www.fbi.gov. Ecco che abbiamo l'inizio di una tabella di corrispondenze, qui sotto. Possiamo già provare a effettuare sostituzioni nel testo cifrato e vedere se salta fuori qualcosa che inizia a somigliare a un testo in inglese. Sarà un semplice cifrario a sostituzione? Presto per dirlo. Ma abbiamo già basi su cui lavorare e arrivare alla soluzione è solo questione di tempo.

Il secondo cifrario è dello stesso tipo: si capisce perché hanno la stessa struttura. Le "parole" cifrate sembrano avere la lunghezza e la collocazione di parole vere. Anche qui c'è quello che sempre essere parte di un indirizzo web: AGJ.OIL/PICB.QNT. Anzi, non proprio un indirizzo a una pagina, ma a un file, dotato di estensione. Ragioniamo: probabile che sia una immagine. Se è visibile su un sito, potrebbe essere .JPG oppure .PNG. Indizio da cui partire ed eseguire sostituzioni nel cifrario, per vedere dove si va a parare. Anche la prima parola desta sospetti. È molto lunga e termina con un punto esclamativo. Molto spesso i messaggi cifrati pubblicati come sfida a chi li sa risolvere contengono un messaggio di congratulazioni o di complimenti per essere riusciti nell'impresa. "Compliments" non funziona; ha undici lettere. PIKODENHFENJIKM infatti ne ha quindici. "Congratulations" ha quindici lettere, invece. E se funzionasse?

Y = W	A = F	H = B	B = I	M = G	S = O	K = V

:: (de)Cifra che ti passa

Chi di noi ha qualche conoscenza con lo scripting o la programmazione può affrontare il problema anche dal punto di vista dell'automazione della decrittazione e del disvelamento dei messaggi. Uno script che prova una dopo l'altra le combinazioni tra le lettere a partire dall'input del testo cifrato e prova a effettuare sostituzioni sulla base di altri input relativi alle corrispondenze tra lettere che sembrano più probabili. Se ci incammi-

Il cifrario del Killer dello Zodiaco ha rotto la testa ai crittanalisti dell'Fbi per decine di anni. Vuoi provarci? La storia del cifrario si trova sul sito http://xrl.us/bedrmh. La storia del killer, http://www.zodiackiller.com.

niamo su questa strada abbiamo già fatto un passo verso l'attività dei decrittatori e dei crittografi professionisti, che passano metà del tempo con carta e matita, l'altra metà a ragionare matematicamente e la terza metà a programmare le loro scoperte su computer. (OK, tre metà sono troppe, ma ci siamo capiti!). Se viene la passione, i codici iniziano a non bastare più e iniziamo a cercarne di più difficili. Oppure iniziamo a creare codici nostri e li collaudiamo per capire se sono abbastanza robusti, e quali sono i loro punti deboli. A un certo punto scopriamo di avere voglia di sfide ancora più interessanti. Cerchiamo su Internet e scopriamo uno dei codici irrisolti della storia, legato al famigerato Killer dello Zodiaco. Molti anni fa questo serial killer ha smesso di agire e si è ritirato. Nessuno lo ha scoperto. Eppure lui ha lasciato una lettera con allegato un cifrario dentro cui, asseriva, si nasconde il segreto della sua identità. Ci mettiamo, ci proviamo, magari ci viene un'ispirazione. Come neanche con il Superenalotto, il nostro programmino, il nostro cifrario fa cadere un mito. E diventiamo più famosi del Killer dello Zodiaco. In bene, ovvio.

:: La vera soluzione

In un attimo siamo passati dal trovare un cifrario piuttosto facile su Internet all'appassionarci alla materia, specializzarci, cercare software, scriverlo, studiare algoritmi, creare il nostro cifrario, cercarne altri su Internet e via dicendo. Per molti di noi finisce qui. Per qualcuno diventa una curiosità. Per pochi di questi, una passione. Pochissimi di questi ne faranno una professione. Probabilmente uno su centomila di noi è un bravissimo crittanalista e non lo sapeva. Uno che potrebbe lavorare perfino all'Fbi. Uno che potrebbe inviare un curriculum e farsi assumere. Uno capace di identificare il Killer dello Zodiaco, dopo che la stessa Fbi ci si è rotta sopra la testa per niente. Se però partissero direttamente da quello, spaventerebbero quelli che hanno un talento crittografico ma non ci hanno ancora provato. Ecco perché l'Fbi mette cifrari semplici su Internet. Semina. Domani potrebbe raccogliere…

David Nool

LA STRADA PIU' SEMPLICE

Non dormi più la notte a causa dei cifrari dell'Fbi? Non esageriamo! Vai su http://xrl.us/bedqyg e scarica SubCypher. È gratis e in versione Windows e Mac OS X. Facilita la soluzione dei cifrari che abbiamo presentato a inizio articolo. Cifrari che si trovano sul sito Fbi alle pagine http://xrl.us/bedrfy e http://xrl.us/bedrgg. Dalle pagine del sito Fbi si arriva anche a un eccellente saggio sulla base della crittografia, chiamato Analysis of Criminal Codes and Ciphers. Su un altro sito si trova un applet Java che aiuta in modo analogo, alla pagina http://xrl.us/bedrg7.

Con questo piccolo programmino per Windows e Mac OS X i cifrari non richiedono neanche più carta e matita! http://xrl.us/bedqyg. Come si vede, siamo andati avanti nella decifrazione dell'enigma dell'Fbi…

LE PAROLE SONO IMPORTANTI

Microdizionario per aspiranti crittanalisti. Sì, si dice così.

Cifrare = trasformare il testo normale in testo cifrato.
Cifrario = schema di codifica e decodifica del testo.
Crittanalisi = la scienza della crittografia.
Crittografia = l'arte (e la scienza) di scrivere in modo nascosto, ovvero creare cifrari.
Decifrare = trasformare il testo cifrato in testo normale usando una chiave in modo autorizzato.
Decrittare = come decifrare, solo che non siamo autorizzati ad avere una chiave e ce la troviamo da soli!
Quando scrivono "crittare, "criptare", cambia pagina. Gente che non sa scrivere in italiano in chiaro, come farà a saperne di italiano cifrato?

E PER GLI AMANTI DI LINUX…

Per creare un cifrario a sostituzione, semplice semplice ma concreto, basta una riga di shell, per usare il comando tr. Scriviamo:

tr '[abcdefghijklmnoqstvwyz]' '[fideltybravngchkopsuwm]'

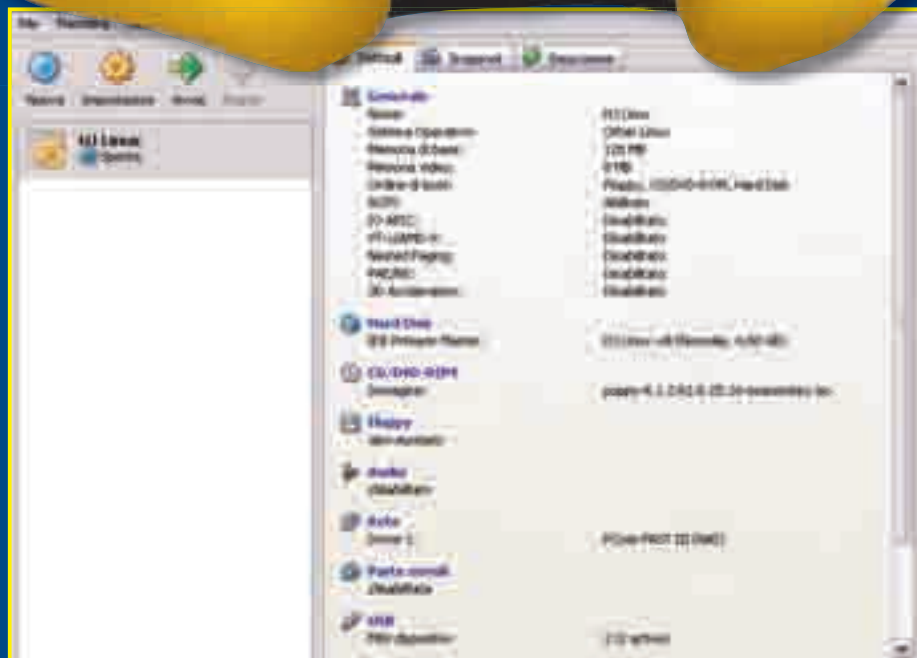
La a della prima stringa viene sostituita dalla f della seconda stringa e così via. Naturalmente la chiave di cifratura deve essere pensata bene, per esempio evitando le sovrapposizioni (una lettera della chiave che ha due significati diversi).

PIÙ LINUX PER TUTTI

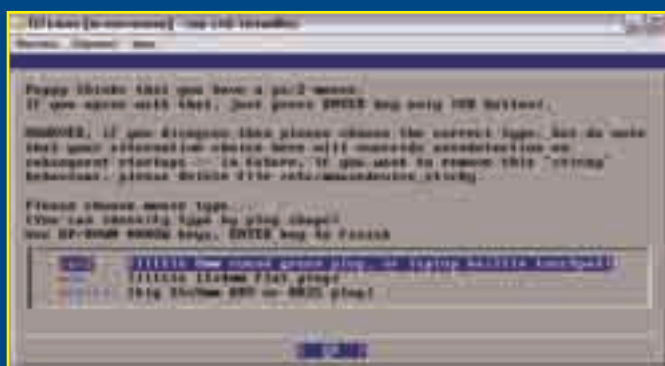
Portiamo sempre con noi Linux su una chiavetta USB

Linux è un sistema operativo complesso e virtualmente infinito: chi è alle prime armi spesso si spaventa di quanto ci sia da leggere e imparare prima di installare per la prima volta una distro del pinguino. Vogliamo provare a sfatare questa comune credenza, dimostrando che Linux può essere un S.O. per tutti e che possiamo imparare a conoscerlo e a usarlo senza toccare la nostra installazione di Windows, sfruttando ciò che la tecnologia ci mette a disposizione.

:: VirtualBOX

Immancabile quando si parla di provare un sistema operativo senza installarlo, VirtualBOX ci permette di creare una macchina virtuale su cui possiamo far girare quello che vogliamo. L'obiettivo rimane comunque la chiavetta USB, ma il PC virtuale di VirtualBOX ci servirà per la prima esecuzione e la successiva installazione di una distribuzione adatta al nostro scopo. Possiamo scaricare gratuitamente l'ultima versione dal sito http://www.virtualbox.org. Dopo averla installata, procediamo con la creazione di una macchina virtuale minimale: non ci servono caratteristiche da top di gamma, basta un computer con RAM e disco sufficienti per poter eseguire Linux e soprattutto che supporti CD e USB.

La schermata di avvio di VirtualBOX, con la macchina virtuale già pronta e configurata.

:: La distro adatta

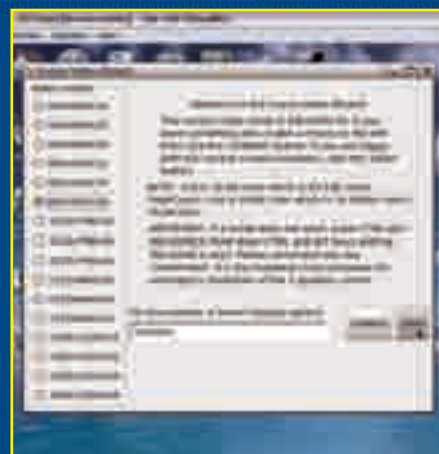
Linux, come sappiamo, è come un pacchetto di caramelle miste: esiste in varie forme e diversi aromi, tutto sta nel scegliere la distribuzione che più si adatta al nostro scopo.
Dato che vogliamo installarlo su una chiavetta USB, magari quella vecchia da un giga che non usiamo più perché non ci sta su più niente, scegliamo una distribuzione leggera e contenuta: Puppy Linux ci pare adatta perché in un'immagine ISO da meno di 100 MB

La configurazione del tipo di mouse e del layout della tastiera durante il boot da immagine CD di Puppy Linux.

è presente il sistema operativo essenziale ma con tutte le più utili funzionalità, come il supporto USB.
Possiamo scaricare le ISO dell'ultima versione disponibile all'indirizzo http://www.puppylinux.org/downloads/official-releases/puppy-linux-412. Tra l'altro è disponibile anche in versione "retro", per poter funzionare su computer ormai datati.

:: Prima esecuzione

Per poter avviare Puppy Linux sulla nostra macchina virtuale, dobbiamo indicare a VirtualBOX che nel lettore CD virtuale deve essere presente l'immagine ISO della distro che abbiamo scaricato.
Facciamo clic sulla dicitura CD/DVD-ROM nella finestra di configurazione di VirtualBOX e indichiamo di caricare l'immagine ISO di Puppy Linux (nel nostro caso puppy-4.1.2-k2.6.25.16-seamonkey.iso). A questo punto possiamo fare clic su Avvia per accendere la macchina virtuale ed eseguire il boot da CD. Puppy avrà bisogno di una minima configurazione iniziale: ha bisogno di sapere che tipo di tastiera montiamo e la modalità grafica che il nostro hardware supporta. Noi ci siamo trovati bene indicando tastiera PS/2 con layout italiano e modalità grafica Xvesa 800x600 a 24 bit.
In realtà Puppy dovrebbe funzionare meglio con Xorg, ma abbiamo visto che questa modalità con VirtualBOX ha dei problemi a partire.
Quando appare la schermata del desktop di Puppy, facciamo clic su quest'ultimo e poi su Cattura per passare il controllo del mouse a VirtualBOX e poter impostare la modalità video desiderata. Per tornare al nostro sistema operativo basta premere il tasto Ctrl di destra. A questo punto dovremmo avere Puppy Linux in esecuzione.

:: Seconda fase

Ora dobbiamo installare Puppy Linux sulla nostra chiavetta USB, per poterlo portare sempre con noi (potremo fare il boot da chiavetta USB e avere la nostra distro Linux su qualunque PC che supporti questa funzione).

Dopo l'impostazione della modalità grafica possiamo iniziare a usare Puppy Linux come se funzionasse su un normale PC.

La procedura è molto semplice: inseriamo la nostra chiavetta in una porta libera e, in Puppy, selezioniamo il comando Menu/Setup/Puppy universal installer. Indichiamo che desideriamo compiere l'installazione su USB flash drive nella finestra di dialogo che viene mostrata, selezioniamo la chiavetta di destinazione (nel nostro caso sdf).

Per l'installazione, per andare sul sicuro, scegliamo la modalità Superfloppy facendo clic sull'icona corrispondente e procediamo con le operazioni necessarie: secondo il caso potremmo dover formattare la chiavetta partizionandola con un file system adatto, ma in genere la procedura di installazione di Puppy procede abbastanza filata.

L'installazione di Puppy su chiavetta USB consiste in pochi passaggi per preparare quest'ultima a riceverlo.

:: Boot da USB

Per poter usare la nostra chiavetta-Linux, dobbiamo disporre di un computer in grado di effettuare il boot da USB.
Questa configurazione, se presente, si trova nel BIOS del PC, ma non tutti la supportano. Inoltre, la modalità di impostazione varia da PC a PC secondo il costruttore della scheda madre, ma se siamo abbastanza fortunati e l'hardware è recente e compatibile con la nostra installazione su chiavetta, avremo la nostra distro Linux sempre in tasca.

AMICO COMPILATORE... TI SCRIVO

Progettare e scrivere programmi per Windows senza spendere un capitale per il compilatore

Scrivere i propri programmi è un'attività che può dare molte soddisfazioni: non solo si impara qualcosa di nuovo ogni volta, ma si ottiene software creato ad hoc per le proprie esigenze. Tuttavia non tutti riescono a superare lo scoglio iniziale: come ci si organizza per iniziare a scrivere programmi in autonomia, tenendo conto del fatto che il budget è cronicamente limitato e che magari si è alle prime armi e non si sa bene da dove iniziare? Ecco una piccola guida che fa proprio al caso di chi vuole cominciare, anche solo per hobby, a scriversi il proprio software.

:: Come si programma

Il processore del computer, che sarà quello che dovrà eseguire il nostro programma una volta che lo avremo scritto, a dispetto della sua potenza non è molto intelligente. Capisce solo interminabili sequenze di 1 e 0, che per facilità di lettura noi unità a base carbonio abbiamo raggruppato in Byte e relativi multipli. Facilità di lettura è un eufemismo: tra leggere 10010000 e leggere 0x90 o 144 c'è poca differenza, se non siamo tra gli iniziati. Ma è così che venivano programmati i primi calcolatori, inserendo le istruzioni e i dati bit per bit, con un interruttore alla volta (o quasi).Oggi le cose sono molto cambiate: abbiamo a disposizione numerosi linguaggi di programmazione, ognuno con le proprie regole e ognuno più o meno facile da imparare secondo il caso, ma soprattutto più facili da scrivere e da leggere rispetto a lunghe sequenze di numeri. Questo però, se da un lato ci facilita i compiti, dall'altro complica un po' i passaggi necessari per ottenere il programma finito e funzionante sul nostro computer. Ciò che scriviamo, infatti, deve essere tradotto da un apposito software, chiamato compilatore, in istruzioni comprensibili alla macchina.

C, Pascal, Basic, Cobol, Prolog, Fortran.... ogni linguaggio ha le sue peculiarità ed è adatto a particolari scopi.

:: Dal sorgente all'eseguibile

Qualunque sia il linguaggio di programmazione scelto, ciò che costituisce il sorgente del nostro programma sono uno o più semplicissimi file di testo, scritti con l'editor che ci è più congeniale. Contrariamente a quanto si può pensare, il compilatore non traduce

Strani dialetti

Su http://www.thefreecountry.com/compilers/index.shtml troviamo un elenco esauriente di tutti i compilatori e gli iterpreti gratuiti disponibili in Rete, anche quelli più inusuali e meno usati e per ogni linguaggio di programmazione. Sapevate che esiste un linguaggio composto solo da simboli aritmetici e un altro invece costituito solo da spazi bianchi?

questi testi nel programma finito, ma crea un passaggio intermedio il cui risultato è ciò che viene detto codice oggetto. Questo è sì comprensibile dalla macchina, ma non è direttamente eseguibile: si tratta infatti dei vari frammenti di codice, ognuno corrispondente a un file del nostro sorgente, che devono ancora essere uniti tra loro. Il programma che si occupa di questo compito, e che verifica tutte le dipendenze andando a recuperare l'eventuale codice di libreria necessario e di unirlo al nostro programma, si chiama linker. L'utilità di questo passaggio intermedio sta nella riusabilità del codice: se scrivo una routine che è una figata, non sto a riscriverla ogni volta, ma la inserisco in una libreria da cui poi vado a prelevarla quando mi serve, e posso quindi usarla in più programmi.

:: Ma come scrivo il codice?

Con un editor, naturalmente, un editor di testo qualunque, fosse anche il Blocco note di Windows (ma ne esistono anche di più spartani).

Questo però può andare bene per semplici programmini tipo "Hello World!", che non hanno bisogno di molto codice. Nel caso di programmi più complessi, tenere le fila del codice sorgente può diventare un vero delirio. Per questo motivo sono nati i cosiddetti IDE (Integrated Development Environment, cioè ambiente di sviluppo integrato). Essi sono costituiti da un potente editor di testo, con funzioni specifiche per il programmatore come il syntax highlighting (che mostra elementi diversi del codice con colori e caratteri diversi per facilitare la lettura) o l'autocompletamento del testo, utile per velocizzare la scrittura, il quale può richiamare direttamente il compilatore e il linker per costruire l'eseguibile. Non solo: in molti casi, negli IDE più evoluti e complessi, avremo a disposizione anche altri strumenti, come un browser per tenere traccia dei file sorgenti e un debugger per correggere gli errori dei nostri programmi.

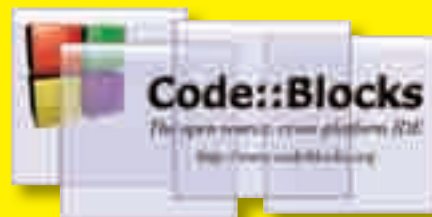
:: Ma quanto costa?

Niente. O meglio, dipende da ciò che vogliamo ottenere: se ci accontentiamo di qualche funzione in meno, possiamo usare IDE open source come Code::Blocks o Visual Studio Express Edition, che sono gratuiti. Se invece vogliamo tutto ma proprio tutto, ma a questo punto abbiamo intenzione di creare programmi seri e poi venderli, allora l'IDE per eccellenza è Visual Studio, che nella sua versione professionale però è parecchio costoso. Quando avremo acquisito abbastanza esperienza, potremo anche destreggiarci con i classici compilatori a riga di comando, come per esempio gcc, che sono tipici dell'ambiente Linux ma che costituiscono anche le origini della programmazione su DOS e su Windows. Sono utili come coltellini svizzeri, possiamo piazzarli su una chiavetta USB con le librerie che ci servono e portarli sempre con noi per ogni esigenza "in trasferta".

Come possiamo iniziare?

I compilatori e gli IDE gratuiti sono numerosi, si trovano facilmente sul Web e spesso non hanno nulla da invidiare a quelli commerciali. Ecco un breve elenco di quelli più usati.

- **Visual Studio 2008 Express Edition**: gratuito da Microsoft, comprende tutti i linguaggi di programmazione di Visual Studio professionale, guide MSDN, documentazione ed esempi; ottimo per imparare a programmare su Windows.
- **Blodshed Dev-C++**: gratuito, open source, con numerose librerie free e open disponibili, non più sviluppato ma facile da usare, con IDE e installer automatico dei pacchetti delle librerie.
- **Code::Blocks**: IDE, multipiattaforma, compatibile con i pacchetti Dev-C++, gratuito e open source.

- **Microsoft Macro Assembler 8.0**: gratuito per uso non commerciale, necessita di Visual C++ 2008 Express Edition; si possono trovare anche versioni precedenti in vari SDK di Microsoft che permettono anche di sviluppare software commerciale.
- **WinAsm**: IDE per scrivere programmi in Assembly per WIndows, supporta Microsoft Macro Assembler.
- **Turbo Delphi Explorer e Turbo Delphi for .NET Explorer**: versioni gratuite di Delphi, ambiente di sviluppo Pascal con IDE di Borland.
- **Free Pascal Compiler**: gratuito e senza IDE, multipiattaforma, supporta Pascal standard e Object Pascal, compatibile con Turbo Pascal.

Ci sono applicazioni per iPhone che lo trasformano in qualcosa di molto diverso. Eccole!

App fa rima con Hack

Ci ricordiamo del diabolico piano di Ra's Al Ghul in "Batman Begins"? Contaminare l'acqua della città con una sostanza che fa impazzire (in senso negativo...) chi la inala. E, dopo che l'acqua tossica si è diffusa per bene nelle condotte, vaporizzarla grazie a un raggio a microonde dando inizio alla conquista. Il concetto di disseminare il germe e poi farlo esplodere è un po' quanto accaduto ad Apple col suo iPhone. Dopo aver venduto oltre 10 milioni di unità, e aver ascoltato altrettanti milioni di lamentele, la casa di Steve Jobs ha svelato l'arma finale: App Store. Il negozio online di software per iPhone/iPod Touch, ha letteralmente fatto esplodere la passione per i due prodotti Apple. Anche quella di programmatori e hacker, i quali, al costo di poche decine di euro, possono acquistare il kit di sviluppo per una piattaforma che, ridendo e scherzando, vanta display multitouch, accelerometro e GPS, oltre a una considerevole potenza di calcolo.

Da qui all'ideazione di migliaia di software il passo è breve. Tanto che, a oggi, se ne contano oltre mezzo milione. Tra videogiochi, programmi "seri" e multimediali, vi sono però alcuni piccoli gioielli che trasformano iPhone in qualcosa di completamente diverso. Che in fondo, a ben pensarci, pur con tutte le costrizioni imposte da Apple (che guadagna una buona fetta dei proventi derivati dalle vendite su App Store), è il concetto stesso di hacking. Vogliamo vedere quali sono i software più "hackerecci", in grado di rivoluzionare iPhone e iPod Touch?

TORCIA: E LUCE FU (GRATUITO)

Come sfruttare la luminosità del display dell'iPhone senza che sia fine a se stessa. E senza sperperare inutilmente la carica della batteria. "Torcia", come dice il nome, una volta avviata fa comparire una schermata bianca grande quanto lo schermo, imposta al massimo la luminosità e disattiva lo spegnimento automatico. Sorpresa: a questo punto l'iPhone diventa una vera e propria torcia luminosa, molto utile nelle situazioni di emergenza. Occhio però a spegnerla dopo averla usata!

WIFI CHECKER: IL TROVA-RETI (GRATUITO)

Fosse a pagamento sarebbe un best-seller, ma la verità è che è gratuito. È un "cacciatore" di reti wireless, che trasforma iPhone in un potente scanner, specializzato nelle reti WiFi gratuite. Fondamentalmente fa il compito già svolto dalla relativa funzione di default del telefono Apple, ma WiFi Checker consente anche di attivare l'Auto-Scan, con relativa frequenza di scansione. Una volta trovata una rete aperta, possiamo decidere di farcelo segnalare tramite un'apposita notifica.

BEEP: IL "DIALER" (0,79 €)

Genialità e semplicità vanno a braccetto: emette i toni DTMF dei numeri telefonici della rubrica, a tutto volume. Così basta avvicinarlo a un telefono fisso per far comporre a quest'ultimo il numero desiderato. Dove sta l'utilità? Al posto di copiare il numero manualmente dalla rubrica del telefono Apple, basta avvicinarlo alla cornetta di quello fisso. In più, iBeep riconosce il paese del numero che si sta chiamando, e non emette i toni del prefisso internazionale, se non necessari.

ISTETHOSCOPE: IL CUORE È OK (GRATUITO)

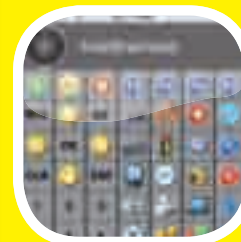
Scarichiamo e installiamo questo programma, colleghiamo le cuffie all'iPhone, e appoggiamo il dispositivo sul cuore o su un'arteria. Ed ecco che, in due secondi, abbiamo per le mani in vero e proprio stetoscopio digitale! iStethoscope, infatti, sfrutta il sensibile microfono di iPhone per rilevare il battito cardiaco e fornirci addirittura il suo diagramma. Un vero e proprio centro diagnostico portatile, per un controllo veloce come per un'analisi più approfondita. Visto cosa si può programmare con un po' di fantasia?

SPEEDTEST: QUANTO CORRI? (GRATUITO)

Siamo incerti sulla velocità di connessione delle reti che utilizziamo? Questo software mette la parola "fine" ai nostri dubbi. Si occupa, infatti, di analizzare le reti UMTS, EDGE e WiFi, rivelandoci la loro effettiva velocità. Visualizzandola in Kbit/sec, e fornendoci anche indicazioni sull'eventuale latenza. Integra inoltre un comodo sistema di archiviazione dei test che permette di confrontare i valori e vedere se rimangono costanti nel tempo entro un certo intervallo prefissato.

BINARKONVERTER: VIA AL BINARIO (GRATUITO)

Un software facile da spiegare a noi hacker, ma che probabilmente è il meno conosciuto e scaricato da App Store. Ovvio, è utile solo a noi.
BinarKonverter si occupa, infatti, di convertire le cifre dal sistema decimale a quello binario e viceversa. Basta scriverlo, premere Convert e la conversione è fatta. L'interfaccia è terribilmente scarna, ha pochissime opzioni, ma è di grande utilità per i programmatori che masticano codice a colazione.

INTELLIREMOTE: L'IPHONE-COMANDO (GRATUITO)

Sfrutta una rete WiFi per mettere in comunicazione iPhone o Touch con un PC basato su Windows. E a questo punto trasforma l'apparecchio di Apple in telecomando, anche senza necessariamente dover utilizzare iTunes. E con un vantaggio mica da poco: basandosi su una rete WiFi non ha i limiti del classico telecomando a raggi infrarossi. Quindi, nessun problema se si è distanti dal PC o se tra noi e il computer c'è un tavolo o qualche ostacolo.